

FIG. 1 (PRIOR ART)

005655.P003

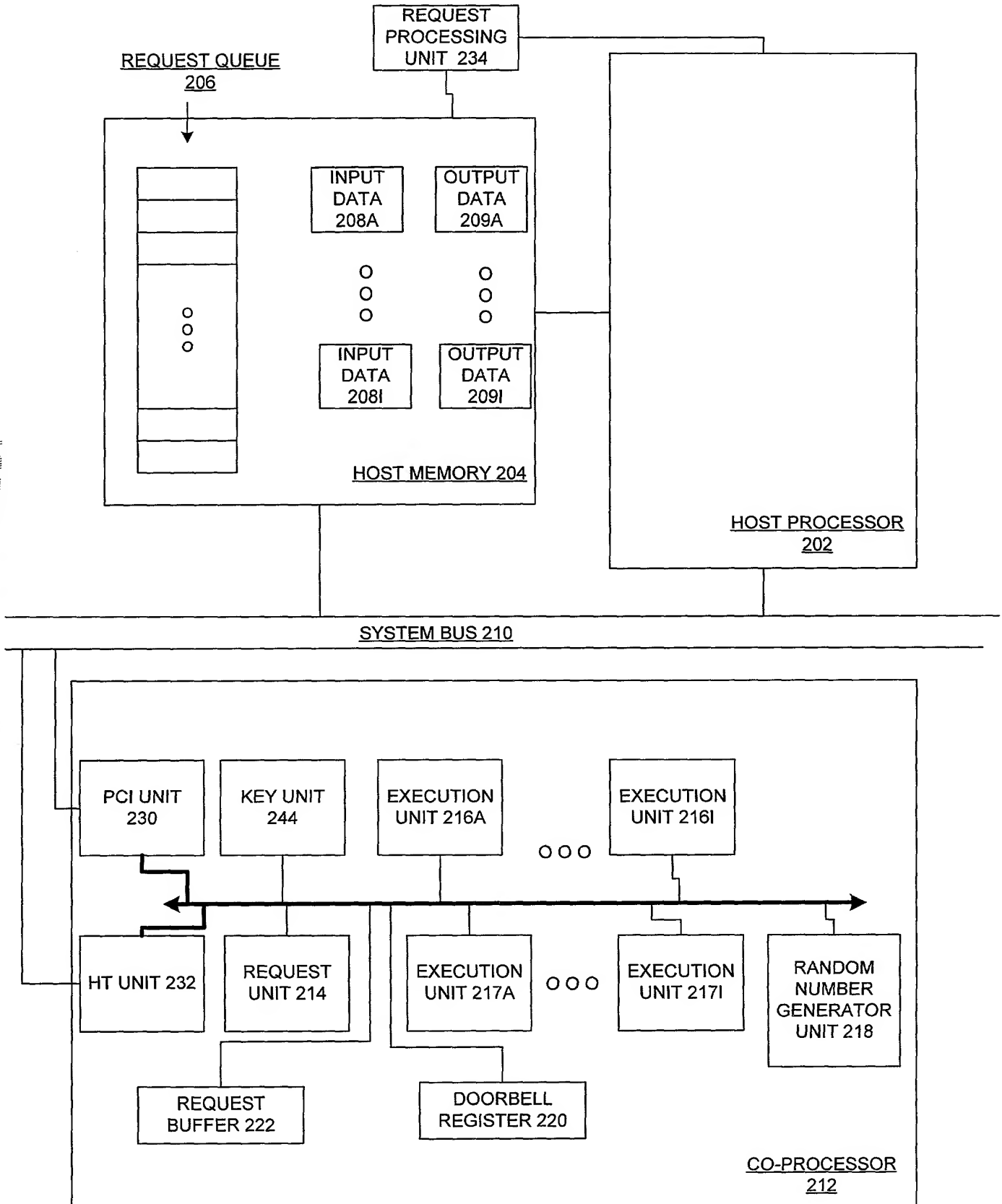
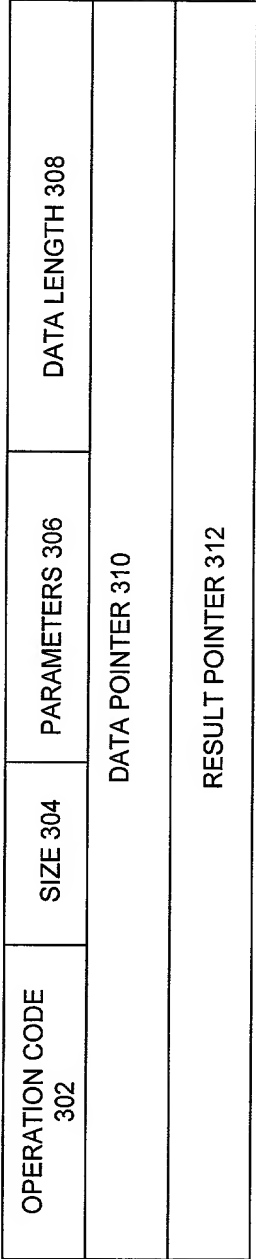


FIG. 2



REQUEST FORMAT
300

FIG. 3

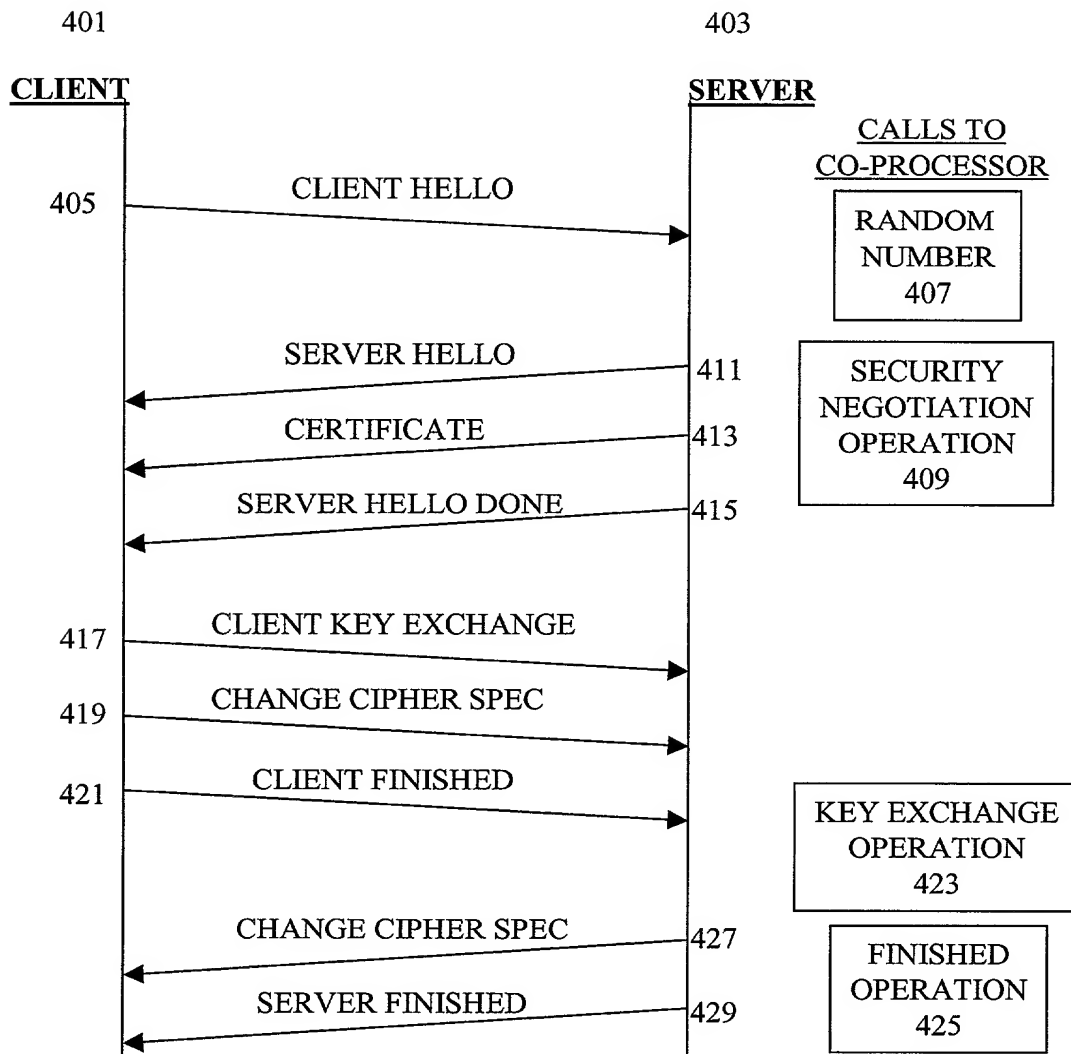


FIG. 4

MACRO SECURITY OPERATIONS	PRIMITIVE SECURITY OPERATIONS
SECURITY NEGOTIATION OPERATION	2 partial hash OPERATIONS (1 MD5 and 1 SHA1)
KEY EXCHANGE OPERATION	1 - RSA OPERATION 20 Hash OPERATIONS (10 MD5 + 10 SHA1) for SSL 3.0 76 Hash OPERATIONS (40 MD5 + 36 SHA1) for SSL 3.1 2 partial hash OPERATIONS (1 MD5 and 1 SHA1)
FINISHED OPERATION	1 - decrypt OPERATION (RC4 or 3DES or DES or AES) 2 - hash OPERATIONS for MAC (either MD5 or SHA1) 4 - hash OPERATIONS (2 MD5 + 2 SHA1) 4 - hash OPERATIONS (2 MD5 + 2 SHA1) 1 - encrypt OPERATION (RC4 or 3DES or DES or AES) 2 - hash OPERATIONS for MAC (either MD5 or SHA1)

FIG. 5

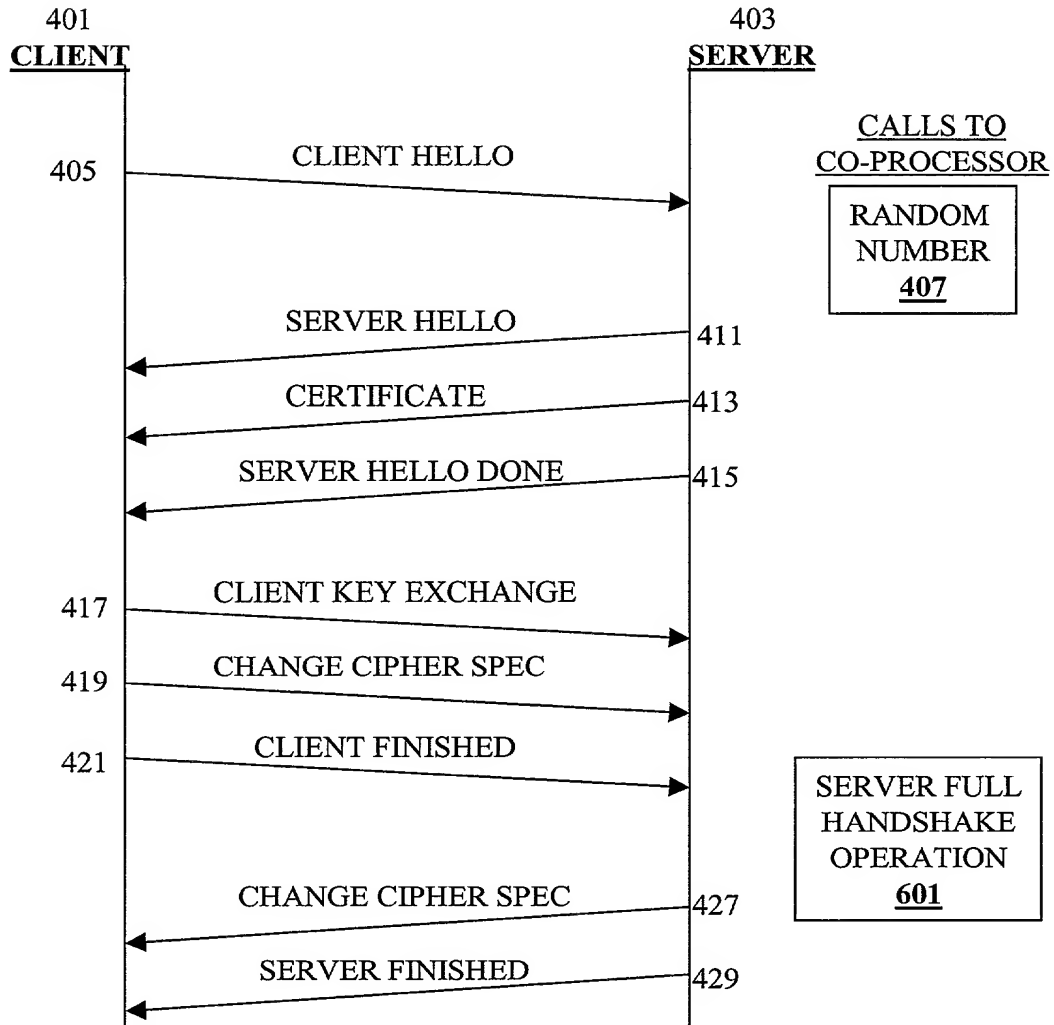


FIG. 6

MACRO SECURITY OPERATION	PRIMITIVE SECURITY OPERATIONS
FULL HANDSHAKE OPERATION	<p>1 - RSA OPERATION</p> <p>20 Hash OPERATIONS (10 MD5 + 10 SHA1) for SSL 3.0</p> <p>76 Hash OPERATIONS (40 MD5 + 36 SHA1) for SSL 3.1</p> <p>6 – hash OPERATIONS (3 MD5 + 3 SHA1)</p> <p>1 – encrypt OPERATION ((A)RC4 or 3DES or DES or AES)</p> <p>6 – hash OPERATIONS (3 MD5 + 3 SHA1)</p> <p>1 - encrypt OPERATIONS ((A)RC4 or 3DES or DES or AES)</p> <p>2 – hash OPERATIONS for MAC (either MD5 or SHA1)</p>

FIG. 7

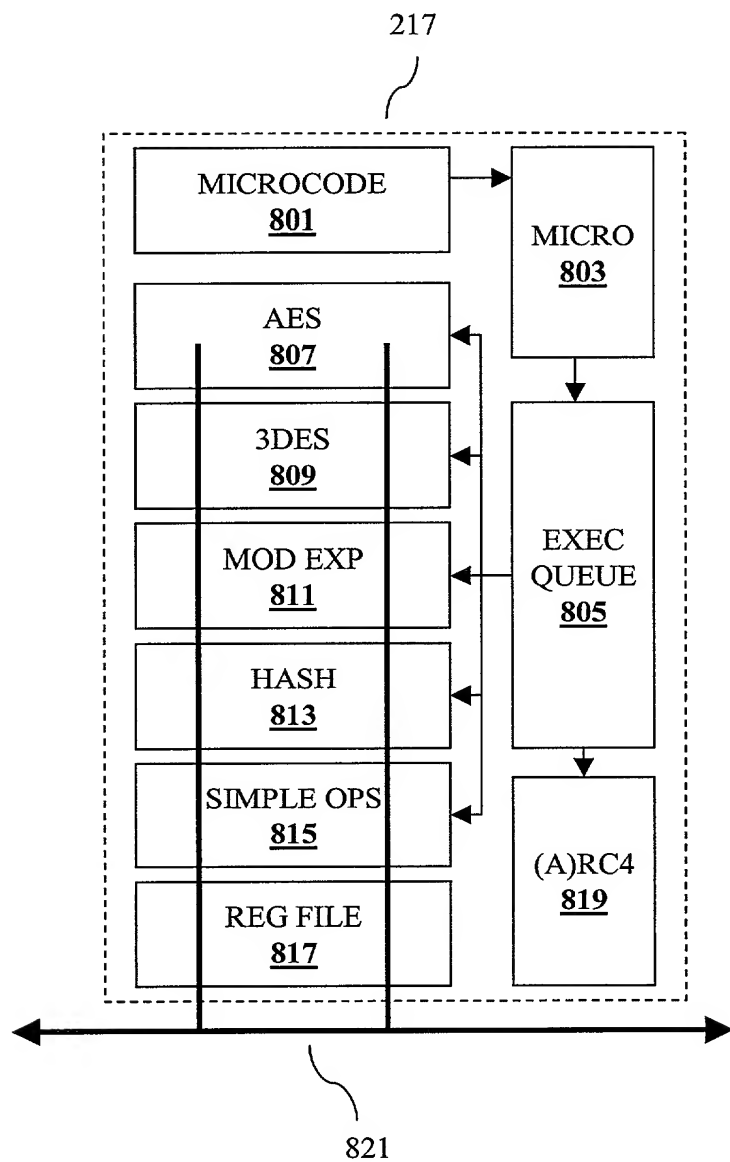


FIG. 8

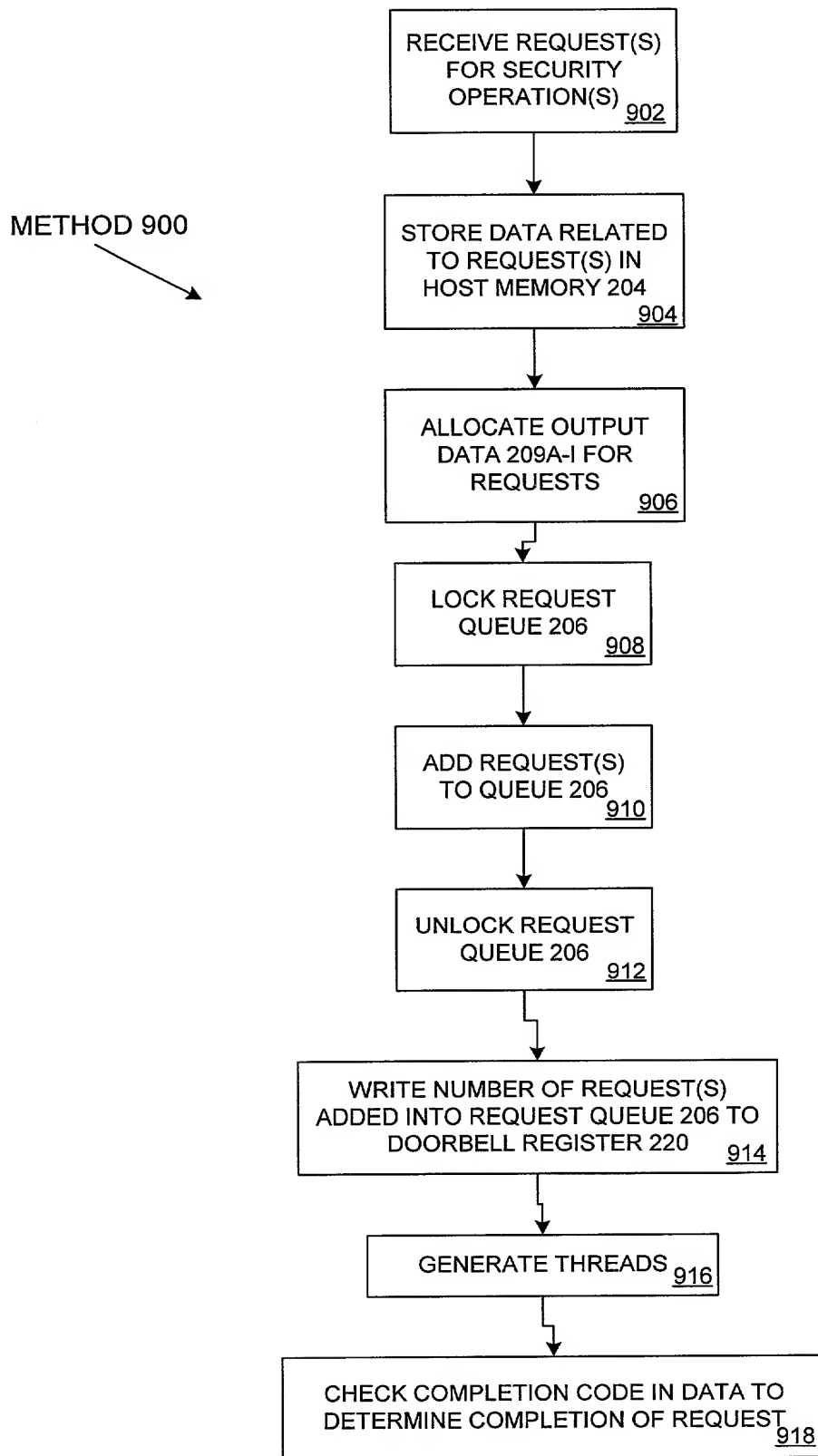


FIG. 9

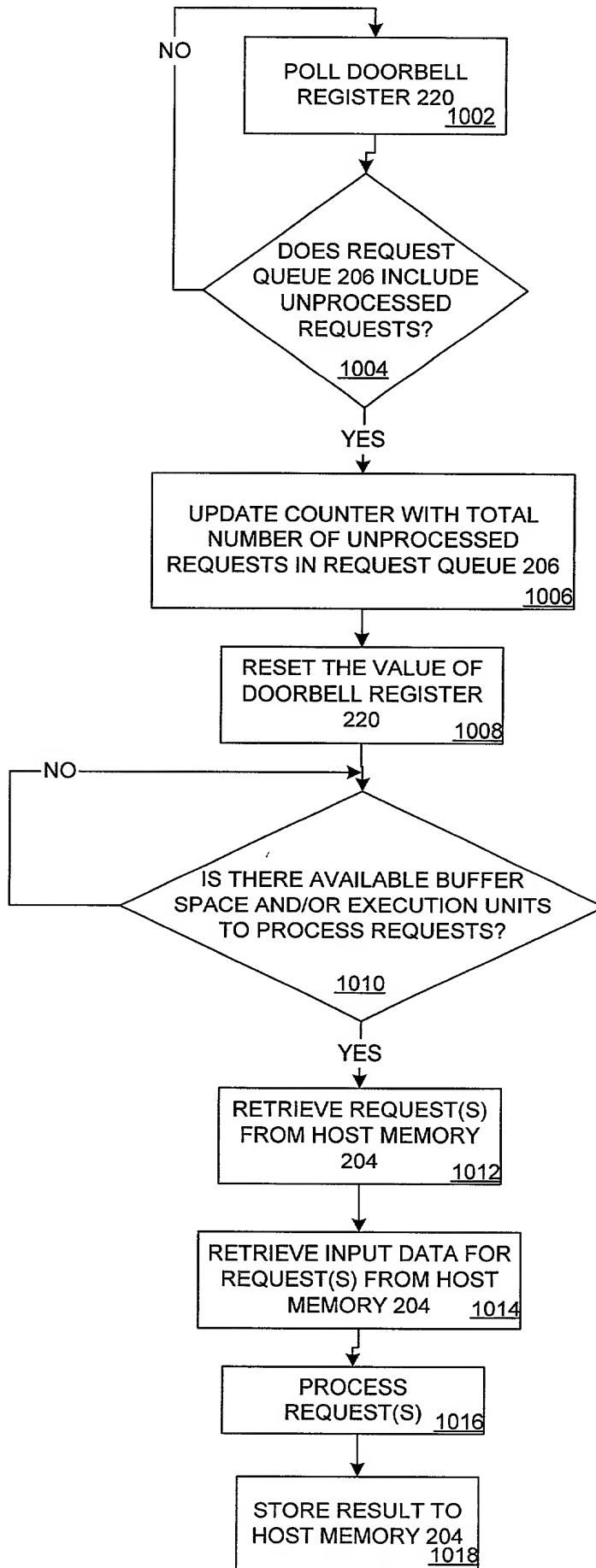


FIG. 10